Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1, 3, 9-11, and 13-29 are pending in the application, with claims 1, 11, and 25 being the independent claims. Claims 2, 4-8 and 12 are sought to be cancelled without prejudice to or disclaimer of the subject matter therein. Claims 1 and 11 are sought to be amended. New claims 23-29 are sought to be added. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Amendments to the Specification

The specification has been amended to correct obvious errors in the discussion of the RC4 stream cipher. A copy of Chapter 17.1 from the book, *Applied Cryptography - Second Edition*, by Bruce Schneier (John Wiley & Sons, Inc., 1996) describing the details of the RC4 stream cipher is attached as an Appendix to this Amendment and Reply. Because a person of skill in the art would recognize the existence of the error in the specification and the appropriate correction, these amendments do not constitute new matter. (*See* MPEP §2163.07(a) citing *In re Odd*, 443 F.2d 1200 (CCPA 1971)).

Rejections under 35 U.S.C. § 112

In the Office Action, claims 1-22 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Without acquiescing to the rejection, the phrase cited by the Examiner in the rejection has been deleted from independent claims 1 and 11 by the above amendment. Thus, the rejection has been rendered moot. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Johns-Vano, European Patent Publication No. EP 0895164 (Vano) in view of Chapter 17 of "Applied Cryptography" by Bruce Schneier (Schneier). Applicants respectfully traverse this rejection.

Independent claims 1 and 11 were amended by the above amendment. The combination of Vano and Schneier does not teach or suggest each and every element of Applicants' amended independent claims 1 and 11. Specifically, the combination does not teach or suggest:

> a hardware-based encryption accelerator configured to execute the RC4 stream cipher, the encryption accelerator including a state memory having a plurality of memory locations; and
>
> a system memory coupled to the system bus arranged to store a secret key array associated with the data ,
>
> wherein the hardware-based encryption accelerator is configured to perform an RC4 shuffling operation using portions of the key array, wherein the shuffling operation is performed concurrently with the receipt of each portion of the key array by the encryption accelerator whereby an initial shuffled pattern of substitution values is

generated via hardware and stored in the plurality of memory locations.

as recited in amended independent claim 1. The combination also does not teach or suggest:

a state machine coupled to the combinational logic block and the state memory array configured to,

initialize via hardware an incrementing pattern of substitution values in the state memory array,

perform a first RC4 shuffling operation using a portion of the key array, wherein the first RC4 shuffling operation is performed concurrently with the receipt of a portion of the key array,

generate a pseudo-random number as a result of a second RC4 shuffling operation;

byte-wise transfer a portion of the data to the combinational logic block as a first input value,

transfer the generated pseudo-random number to the combinational logic as a second input value,

logically operate on the first and second input values by the combinational logic to form a resulting data byte, and outputting the resulting data byte.

as recited in amended independent claim 11. For at least these reasons, amended independent claim 1 and 11 are patentable over the combination of Vano and Schneier. Claims 3, 9, and 10 depend from claim 1 and claims 13-22 depend from claim 11. For at least the above reasons, and further in view of their own features, claims 3, 9, 10, and 13-22 are patentable over the combination of Vano and Schneier. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

New Claims

Applicants have added new claims 23-29. Applicants submit that claims 23-29 are patentable over the cited art. Accordingly, Applicants respectfully requests prompt indication of their allowance.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: June 12, 2006

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600